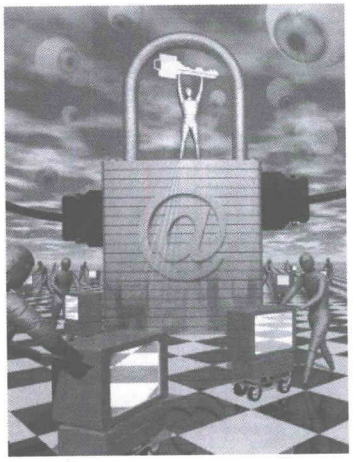
■ ชูสิทธิ์ จูตระกูล

เรียนรู้ โปรโตคอล TCP/IP จาก Network Monitor



ใช้โปรแกรม Network Monitor ศึกษาการทำงานของโปรโตคอล TCP/IP

การเรียนรู้โปรโตคอลต่าง ๆ ในระบบเน็ตเวิร์กส่วนใหญ่เป็นการเรียนรู้ในเชิงทฤษฎี ซึ่งบางครั้งยากต่อการทำความเข้าใจ หรือแม้กระทั่งในห้องเรียน ผู้เรียนไม่สามารถนึกคำถามมาถามวิทยากรเพื่อให้ตัวเองเข้าใจการทำงานของโปรโตคอลได้มากขึ้น ทั้งนี้สาเหตุหนึ่งเกิดจากการที่ไม่ได้เห็นภาพจริงของการทำงานของโปรโตคอล เปรียบได้กับสุภาษิตไทยที่ว่า "สิบปากว่าไม่เท่าตาเห็น สิบตาเห็นไม่เท่ามือสัมผัส (คลำ)" และเมื่อคุณเข้าใจการทำงานของโปรโตคอล รู้ว่าขณะทำงานโปรโตคอลมีการส่งข้อมูลโต้ตอบกันอย่างไร คุณสามารถนำความรู้นี้ไปพัฒนาเป็นโปรแกรมประยุกต์ใช้งานได้ เป็นต้นว่า Web Server, Mail Server หรืออาจจะใช้พัฒนาเป็นโปรแกรมประยุกต์ที่ยังไม่มีใครเขียนมาก่อน ซึ่งในประเทศไทยนับว่าขาดบุคลากรทางด้านนี้มากทีเดียว

ในบทความนี้ผมจะแนะนำให้คุณลองใช้โปรแกรม Network Monitor ศึกษาการทำงานของโปรโตคอล TCP/IP ว่ามีลักษณะแพ็กเกตเป็นอย่างไร มีการ Encapsulation อย่างไร มีการโต้ตอบกันอย่างไร แต่ถ้าคุณมีเครื่องมือ Protocol Analyzer คุณสามารถวิเคราะห์โปรโตคอลต่าง ๆ ได้ดีกว่า แต่ราคาของเครื่องมือตัวนี้มีราคาหลายแสนบาททีเดียว

Network Monitor เป็นโปรแกรมที่ช่วยให้คุณสามารถตรวจจับ วิเคราะห์ และแก้ไขปัญหาที่เกิดในระบบ LAN คุณสามารถที่จะทราบลักษณะรูปแบบของ network traffic และปัญหาในเน็ตเวิร์กได้ รูปที่ 1 แสดงหน้าตาของโปรแกรม Network Monitor

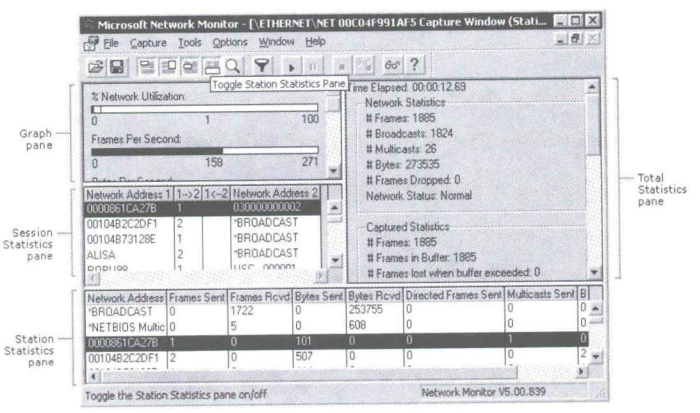
ความสามารถของโปรแกรม Network Monitor

- สามารถจับ เฟรม (packet) โดยตรงจากเน็ตเวิร์ก
- แสดง กรอง บันทึก และพิมพ์ค่าของเฟรมที่ตรวจจับได้

การติดตั้งโปรแกรม Network Monitor

โปรแกรม Network Monitor เป็นโปรแกรมที่มีมาพร้อมกับระบบปฏิบัติการ Windows NT และระบบปฏิบัติการ Windows 2000

การติดตั้งโปรแกรม Network Monitor บนระบบปฏิบัติการ Windows 2000 Server ทำได้ดังนี้



รูปที่ 1 โปรแกรม Network Monitor

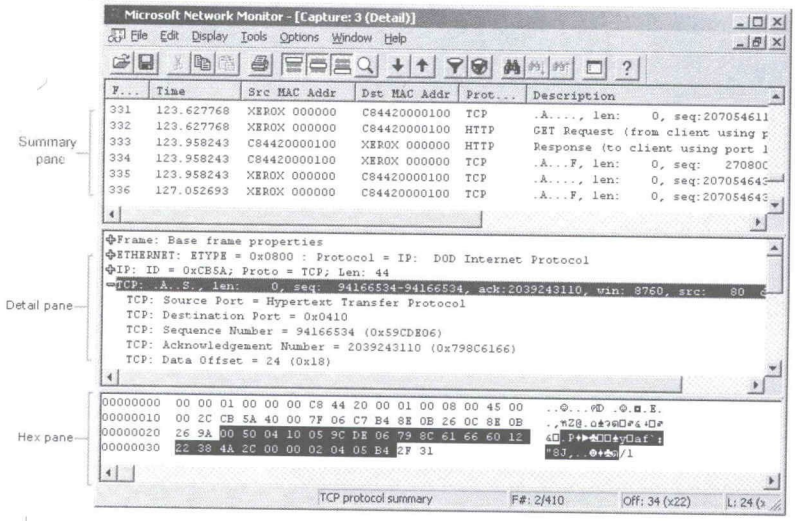
Start —> Settings —> Control Panel —> Add / Remove Programs —> เลือก Add / Remove Windows Components —> คลิกปุ่ม Components และที่หน้าต่างของ Windows Components Wizard —> คลิกที่ Management and Monitoring Tools —> คลิกปุ่ม Details...—> คลิกที่ Check box ของ Network Monitor Tools ดังรูปที่ 3 —> คลิกปุ่ม OK —> คลิก ปุ่ม Next —> กรณีคุณมีการติดตั้ง Terminal Service ไว้ก่อนหน้านี้ จะมีหน้าต่างให้เลือกตอบ Remote administration mode หรือ Application server mode จากนั้นให้ใส่แผ่น CDROM ของระบบปฏิบัติการ Windows 2000 —> คลิกปุ่ม Finish —> คลิกปุ่ม Close และเมื่อติดตั้งเสร็จจะปรากฏไอคอนของ Network Monitor ที่ Group Administrative Tools

การติดตั้งโปรแกรม Network Monitor บนระบบปฏิบัติการ Windows NT Server 4.0 ทำได้ดังนี้

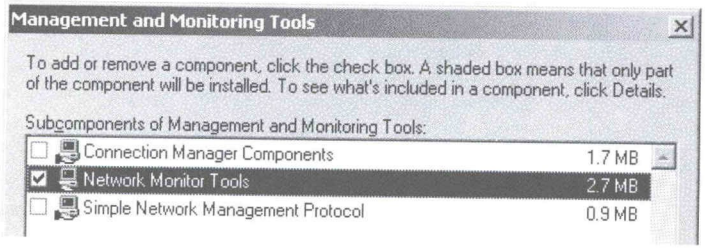
Start —> Settings —> Control Panel —> Network —> เลือก Tab Service —> คลิกปุ่ม Add —> Network Monitor Tools and Agent —> ใส่แผ่น CDROM ของ Windows NT Server 4.0 —> คลิกปุ่ม Close —> Restart เครื่อง และเมื่อติดตั้งเสร็จจะปรากฏไอคอนของ Network Monitor ที่ Group Administrative Tools

การใช้โปรแกรม Network Monitor ตรวจจับแพ็กเกต

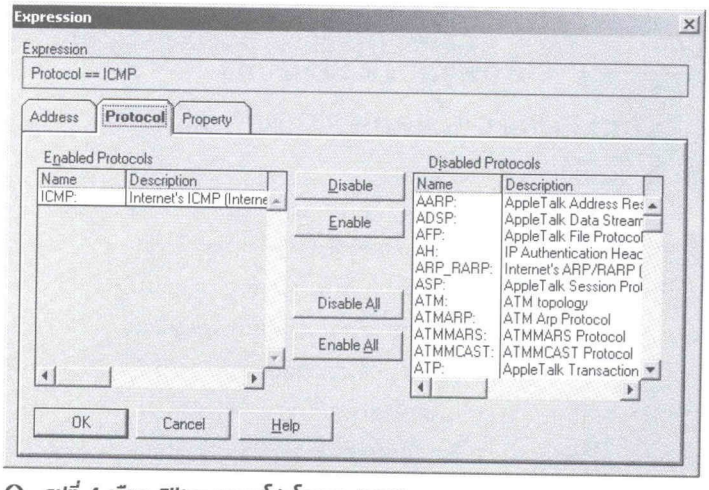
จากเมนู Capture ของโปรแกรม Network Monitor ให้เลือก Start จากนั้นโปรแกรม Network Monitor จะทำการ Capture ทุกแพ็กเกตที่ส่งมาถึงเครื่องที่ติดตั้งโปรแกรม Network Monitor การ Capture จะไม่เลือกว่าเป็นแพ็กเกตของโปรโตคอลใด และสามารถตรวจจับแพ็กเกตที่อุปกรณ์หรือเครื่องคอมพิวเตอร์ทำการ Broadcast ออกมาในระบบเครือข่ายได้ ถ้าคุณต้องการศึกษาว่าฟังก์ชันการทำงานของแต่ละโปรโตคอลทำงานอย่างไร ให้คุณเรียกใช้งานฟังก์ชันนั้น เป็นต้นว่าใช้คำสั่ง Ping เพื่อศึกษาการทำงานของโปรโตคอล ICMP, ARP หลังจากนั้นให้หยุดการ Capture ข้อมูลโดยเลือก Stop หรือ Stop and view จากเมนู Capture จากนั้นคุณก็สามารถเรียกดูรายละเอียดของแต่ละแพ็กเกตได้ และคุณสามารถใช้การ Filter เลือกดูเฉพาะโปรโตคอลหรือเฉพาะแพ็กเกตที่ส่งโต้ตอบระหว่างเครื่อง A กับเครื่อง B โดยการเลือก Filter... จากเมนู Capture ดังรูปที่ 4 และรูปที่ 5



รูปที่ 2 แสดงแพ็กเกตของโปรโตคอล TCP/IP ที่ Capture ได้



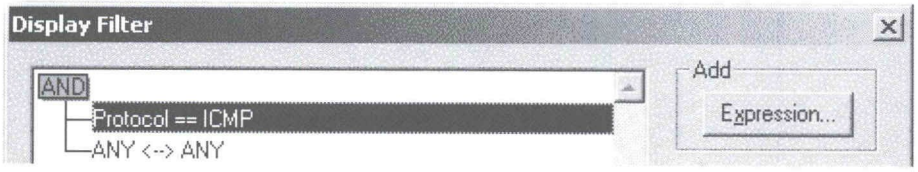
รูปที่ 3 เลือกติดตั้ง Network Monitor Tools



รูปที่ 4 เลือก Filter เฉพาะโปรโตคอล ICMP

พื้นฐานโปรโตคอล TCP/IP

โปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นชุดของโปรโตคอลหลายตัวที่ช่วยกันทำงาน โปรโตคอลที่สำคัญก็คือ TCP, UDP, IP, ARP และ ICMP รูปที่ 6 แสดงชุดโปรโตคอลของ TCP/IP ในแต่ละ Layer



รูปที่ 5
เงื่อนไขการ Filter เฉพาะโปรโตคอล ICMP โดยไม่ระบุว่ามาจากเครื่องใด

โปรโตคอล TCP (Transmission Control Protocol) เป็นโปรโตคอลที่มีความเชื่อถือได้ในการส่งผ่านข้อมูล มีการตรวจสอบว่าข้อมูลถึงผู้รับหรือไม่ ถ้าไม่ถึงจะทำการส่งข้อมูลไปใหม่ ตัวอย่าง Service ที่ใช้บริการโปรโตคอล TCP เช่น Telnet, FTP, HTTP

โปรโตคอล UDP (User Datagram Protocol) เป็นโปรโตคอลที่ไม่เน้นเรื่องความน่าเชื่อถือในการส่งข้อมูล แต่เน้นทางด้านความเร็ว ความง่ายในการทำงาน ตัวอย่าง Service ที่ใช้บริการโปรโตคอล UDP เช่น DNS, TFTP, SNMP

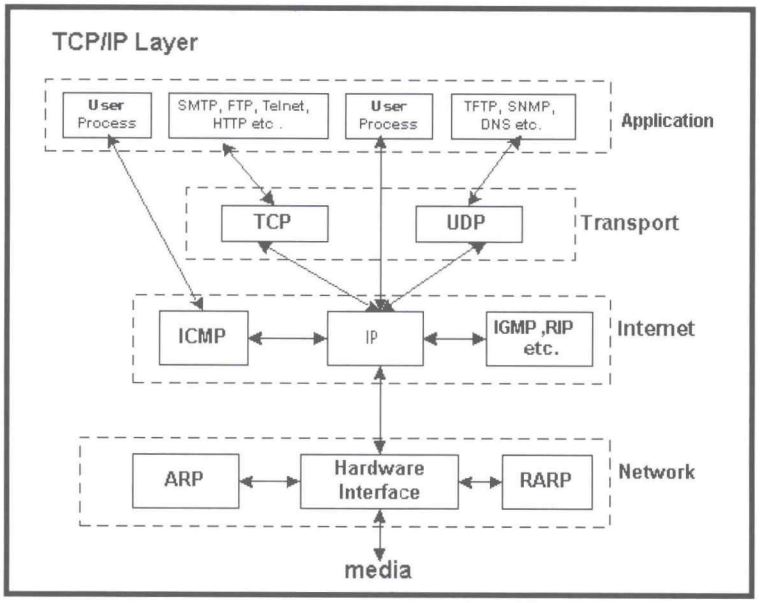
โปรโตคอล IP (Internet Protocol) เป็นโปรโตคอลสำคัญที่ทำหน้าที่ห่อหุ้มโปรโตคอล TCP หรือ UDP เพื่อไปส่งให้แก่ผู้รับ ซึ่งในระหว่างทางอาจผ่านอุปกรณ์หลายอย่างเช่น เราเตอร์ สวิตชิง บางครั้งแพ็กเกตอาจถูกแบ่งย่อย ๆ แล้วส่งผ่านอุปกรณ์ และจะไปทำการรวมแพ็กเกตย่อยกันใหม่เป็นแพ็กเกตรูปแบบเดิม

โปรโตคอล ICMP (Internet Control Message Protocol) เป็นโปรโตคอลที่ช่วยให้โปรโตคอลอื่นในชุด TCP/IP ทำงานได้ดีขึ้น ช่วยในการรายงานข้อผิดพลาดต่าง ๆ

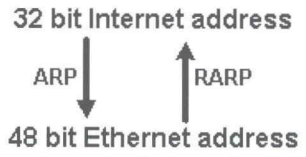
โปรโตคอล ARP (Address Resolution Protocol) เป็นโปรโตคอลที่ช่วยในการหาค่า Hardware Address ของเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ต่าง ๆ โดยใช้เลข IP Address เพื่อถามหาค่าของ Hardware Address

โปรโตคอล RARP (Reverse Address Resolution Protocol) เป็นโปรโตคอลที่ช่วยในการหาค่า IP Address ของเครื่องคอมพิวเตอร์ โดยใช้ Hardware Address เพื่อถามหาค่าของ IP Address ทำงานตรงข้ามกับ ARP

เราจะมา Capture โปรโตคอล ARP เพื่อดูรายละเอียดของโปรโตคอลว่าประกอบด้วยค่าอะไรบ้าง ลักษณะการทำงานเป็นอย่างไรโดยใช้โปรแกรม Network Monitor แต่ก่อนอื่นผมขออธิบายลักษณะของโปรโตคอล ARP ก่อนเพื่อจะได้เข้าใจเมื่อดูแพ็กเกตของ ARP ที่ Capture มาได้



รูปที่ 6 TCP/IP Layer และชุดโปรโตคอลต่าง ๆ ของ TCP/IP



รูปที่ 7
แสดงหน้าที่ของ ARP และ RARP

โปรโตคอล ARP (Address Resolution Protocol)

เมื่อเครื่องคอมพิวเตอร์สองเครื่องติดต่อสื่อสารกันในระบบ LAN โดยการใช้โปรโตคอล TCP/IP เครื่องคอมพิวเตอร์ทั้งสองจะใช้ Hardware Address (หรือ Mac Address) เป็นตัวอ้างถึงเครื่องคอมพิวเตอร์แต่ละเครื่อง ซึ่ง Mac Address ในที่นี้จะหมายถึง เลขฐานสิบหกจำนวนสิบสองหลักที่อยู่บน Network Card นั่นเอง การติดต่อสื่อสารกันระหว่างเครื่องจะทำใน Layer ล่างซึ่งเป็น Layer ของเน็ตเวิร์กจึงต้องอาศัยเลขประจำตัวของ Network Card ในการสื่อสารกัน ส่วนผู้ใช้งานทำงานอยู่ใน Layer Application ซึ่งเป็น Layer ที่อยู่บนสุดเมื่อต้องการจะติดต่อสื่อสารกับเครื่องคอมพิวเตอร์อีกเครื่องจะใช้ Mac Address ก็จำยาก ไม่สื่อความหมายอะไรและที่สำคัญคือจัดเป็นกลุ่มได้ยาก ไม่รู้จะใช้อะไรเป็นตัวบ่งบอกว่าเครื่องนั้นอยู่ด้านใดของเราเตอร์ ซึ่งการจะเก็บ

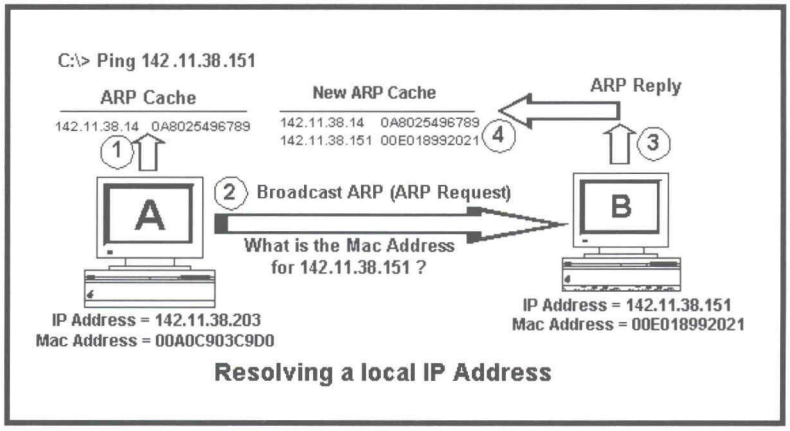
ค่าเหล่านี้ไว้ในตัวเราเตอร์เองก็จะทำให้เกิดความล่าช้าขึ้น จึงได้สมมติเลขที่จำง่าย มีความหมายในตัวขึ้นมาซึ่งเรียกว่า IP Address เครื่องคอมพิวเตอร์ทุกเครื่อง รวมทั้งอุปกรณ์คอมพิวเตอร์ทุกตัวถ้าต้องการติดต่อสื่อสารกันโดยใช้โปรโตคอล TCP/IP นั้นต้องมีเลข IP Address ประจำทุกเครื่องและห้ามซ้ำกัน ดังนั้นถ้านาย A ทำงานที่เครื่อง IP Address 142.11.38.203 ต้องการจะติดต่อกับ Web Server ที่มี IP Address 142.11.38.151 จะใช้คำสั่ง http://142.11.38.151/index.htm แต่เครื่องที่นาย A ใช้งานอยู่และ Web Server ไม่รู้จะติดต่อกันอย่างไรรู้แต่ค่า IP Address ของแต่ละเครื่อง โปรโตคอล ARP จะมาช่วยแก้ปัญหานี้โดยการส่ง Broadcast ไปถามในเน็ตเวิร์กว่าเครื่องใดที่มี IP Address เป็น 142.11.38.151 ให้บอก Mac Address มาด้วย และเมื่อเครื่อง Web Server ได้รับ ARP Request ก็จะใส่ Mac Address ของตัวเองลงใน ARP Reply ส่งกลับไปบอกเครื่องนาย A หลังจากนั้นเครื่องนาย A ก็จะนำ Mac Address ใส่ลงไปใน TCP Packet เพื่อส่งไปยังเครื่อง Web Server ต่อไป

ขั้นตอนการทำงานของโปรโตคอล ARP กรณีเครื่องทั้งสองอยู่ใน Network Address เดียวกัน

ขั้นตอนที่ 1 จากรูปที่ 8 เมื่อมีการใช้คำสั่ง Ping 142.11.38.151 จากเครื่อง IP Address 142.11.38.203 จะมีการตรวจสอบ IP Address ของเครื่องปลายทาง (142.11.38.151) ว่าอยู่ใน Network Address เดียวกันกับเครื่อง IP Address 142.11.38.203 หรือไม่ ถ้าอยู่ใน Network Address เดียวกัน จะทำการตรวจสอบ Mac Address ของเครื่องปลายทางจาก ARP Cache ที่อยู่ในหน่วยความจำของเครื่อง 142.11.38.203

ขั้นตอนที่ 2 ถ้าหา Mac Address ของเครื่องปลายทางจาก ARP Cache ไม่พบ เครื่อง 142.11.38.203 จะทำการส่ง Broadcast ARP Request ออกไปถามเครื่องต่าง ๆ ในเน็ตเวิร์กว่าเครื่องใดที่มี IP Address เป็น 142.11.38.151 มี Mac Address เป็นเลขใด และในแพ็กเกตของ ARP ที่ส่งไปถามจะใส่เลข IP Address (142.11. 38.203) และ Mac Address (00A0C903C9D0) ของมันอยู่ด้วย เมื่อเครื่อง 142.11.38.151 ได้รับ ARP Request จะทำการสร้าง ARP Reply แล้วใส่เลข Mac Address (00E018992021) เลข IP Address (142.11.38.151) ลงไปด้วย แล้วทำการส่งกลับไปที่เครื่อง IP Address 142.11.38.203

ขั้นตอนที่ 3 message ที่ตอบรับนี้ จะส่งตรงไปที่ Mac Address ของเครื่อง IP Address 142.11.38.203 เฉพาะเครื่อง 142.11.38.203 เท่านั้นที่ทำการตอบรับ เครื่องอื่น ๆ จะไม่สนใจต่อการตอบรับนี้



รูปที่ 8 แสดงการทำงานของโปรโตคอล ARP (Network Address เดียวกัน)

ขั้นตอนที่ 4 เมื่อเครื่อง IP Address 142.11.38.203 ได้รับ message ตอบรับแล้วจะทำการเพิ่ม Mac Address และ IP Address ของเครื่อง 142.11.38.151 ลงใน ARP Cache ของตัวเองการสื่อสารจะเริ่มเกิดขึ้นหลังจากนี้

ขั้นตอนการทำงานของโปรโตคอล ARP กรณีเครื่องทั้งสองอยู่ต่าง Network Address กัน

ขั้นตอนที่ 1 จากรูปที่ 9 เมื่อมีการใช้คำสั่ง Ping 10.1.1.1 จากเครื่อง IP Address 142.11.38.203 จะมีการตรวจสอบ IP Address ของเครื่อง 10.1.1.1 ว่าอยู่ใน Network Address เดียวกันกับเครื่อง 142.11.38.203 หรือไม่ ปรากฏว่าอยู่คนละ Network Address ดังนั้นจะทำการตรวจสอบเส้นทางที่จะไปติดต่อกับเครื่อง 10.1.1.1 โดยดูจาก local route table ที่อยู่ในหน่วยความจำของเครื่อง 142.11.38.203 ถ้าพบเส้นทาง จะทำการหา Mac Address ของ Gateway จาก ARP Cache (การหาเส้นทางจะเป็นหน้าที่ของเราเตอร์ และการใช้โปรโตคอล Routing แบบ OSPF จะช่วยให้การหาเส้นทางมีประสิทธิมากกว่าใช้โปรโตคอล Routing แบบ RIP และจะช่วยลด Traffic ภายในเน็ตเวิร์กด้วย)

ขั้นตอนที่ 2 ถ้าไม่พบเส้นทาง จะใช้โปรโตคอล ARP ไปหา Mac Address ของ Default Gateway เนื่องจากสิ่งเดียวที่รู้ขณะนี้คือ เครื่อง 10.1.1.1 เป็นเครื่องที่อยู่คนละ Network Address ซึ่งต้องใช้เราเตอร์เป็นตัวเชื่อมกับเครื่อง 10.1.1.1

ขั้นตอนที่ 3 เราเตอร์จะตอบ Mac Address ของตัวเราเตอร์เองไปให้เครื่อง 142.11.38.203 และเครื่อง 142.11.38.203 จะใช้ ICMP ทำการส่ง echo ไปให้แก่เราเตอร์ และตัวเราเตอร์จะทำการส่ง echo ไปให้เครื่อง 10.1.1.1 (ตัวเราเตอร์จะมีค่า Mac Address ของเครื่องที่ต่ออยู่กับเราเตอร์ โดยอาศัยดูจาก Cache หรือดูจากการ Broadcast หรือหา Mac Address ของเครื่องต่าง ๆ)

ขั้นตอนที่ 4 เครื่องปลายทาง 10.1.1.1 จะตอบกลับด้วย ICMP echo แต่เพราะเครื่อง 142.11.38.203 อยู่คนละเน็ตเวิร์ก การตอบนี้จะส่งไปที่เราเตอร์ และเราเตอร์จะส่งต่อไปให้แก่เครื่อง 142.11.38.203

ARP Cache

ARP Cache เป็นตารางที่ใช้เก็บค่าความสัมพันธ์ของ IP Address และ Mac Address โดย ARP Cache นี้เก็บอยู่ในหน่วยความจำของเครื่องที่ใช้โปรโตคอล TCP/IP เมื่อมีการติดต่อสื่อสารกับเครื่องอื่นมันจะทำการตรวจสอบค่า Mac Address จาก ARP Cache ก่อนเสมอ ถ้าไม่พบ Mac Address นั้น จะทำการ Broadcast ARP ไปในเน็ตเวิร์กเพื่อที่จะหา Mac Address (Hardware Address) เมื่อพบแล้วมันจะเก็บค่าใหม่นี้ลงใน ARP Cache เพื่อประโยชน์ในการติดต่อครั้งต่อไป ARP Cache จะช่วยให้ทราฟฟิกในเน็ตเวิร์กลดลงเพราะถ้าพบค่า Mac Address จาก ARP Cache ก็ไม่ต้องส่ง ARP ไปในเน็ตเวิร์กและ ARP Cache จะมีการกำหนดให้หมดอายุ จะได้สร้าง ARP Cache ใหม่เพื่อให้ได้ค่าที่ทันสมัยอยู่ตลอดเวลา (เครื่องคอมพิวเตอร์ในเน็ตเวิร์กอาจเปลี่ยน IP Address เป็นเลขอื่น ซึ่งจะทำให้ความสัมพันธ์ระหว่าง IP Address และ Mac Address ที่เก็บอยู่ใน ARP Cache ไม่ถูกต้อง)

ตัวอย่างของ ARP Cache

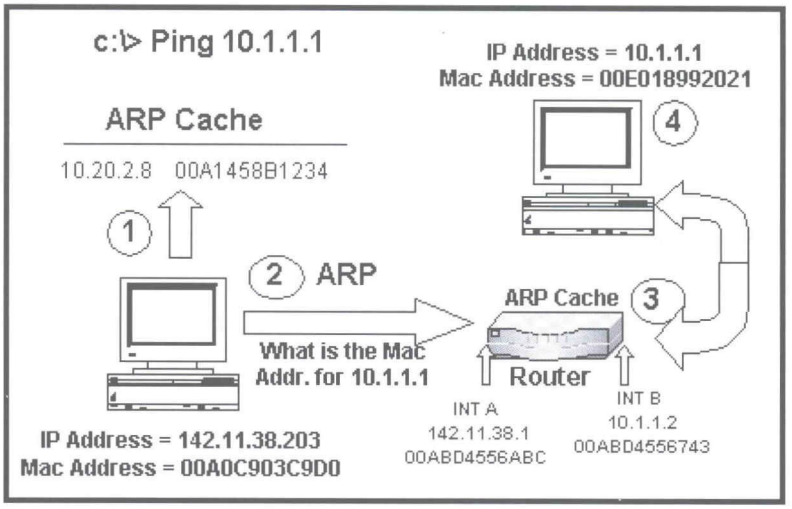
```
C:\>arp -a
Interface: 142.11.38.83 on Interface 0x2
Internet Address      Physical Address      Type
142.11.38.8           00-80-c8-e6-39-fe     dynamic
142.11.38.203         00-a0-c9-03-c9-d0     dynamic
```

รูปแบบของโปรโตคอล ARP

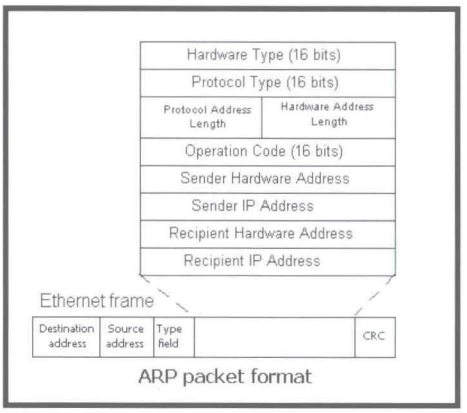
โปรโตคอล ARP ไม่สามารถส่งออกไปในเน็ตเวิร์กได้โดยตรง แต่จะต้องถูกห่อหุ้มอยู่ใน Ethernet Frame ดังรูปที่ 10

โปรโตคอล ARP มีรายละเอียดดังนี้

- Hardware Type มีขนาด 16 บิต บอกประเภท Hardware ของระบบเครือข่ายที่ใช้ในการส่งโปรโตคอล ARP ในที่นี้ใช้ 1 ซึ่งหมายถึง Ethernet 10 Mb
- Protocol Type มีขนาด 16 บิต บอกถึงโปรโตคอลในระดับบนที่เรียกใช้บริการนี้ ในที่นี้คือโปรโตคอล IP ซึ่งมีค่าเป็นเลขฐาน 16 เท่ากับ 0800
- Hardware Address Length มีขนาด 8 บิต ใช้ในการระบุความยาวของ Hardware Address มีหน่วยเป็นไบต์ ในที่นี้คือ Ethernet Address มีค่าเท่ากับ 6 (เลขฐานสิบ)
- Protocol Address Length มีขนาด 8 บิต ใช้ในการระบุความยาวของ Protocol Address มีหน่วยเป็นไบต์ ในที่นี้คือ IP Address มีค่าเท่ากับ 4 (เลขฐานสิบ)



รูปที่ 9 การทำงานของโปรโตคอล ARP (Network Address ต่างกัน)



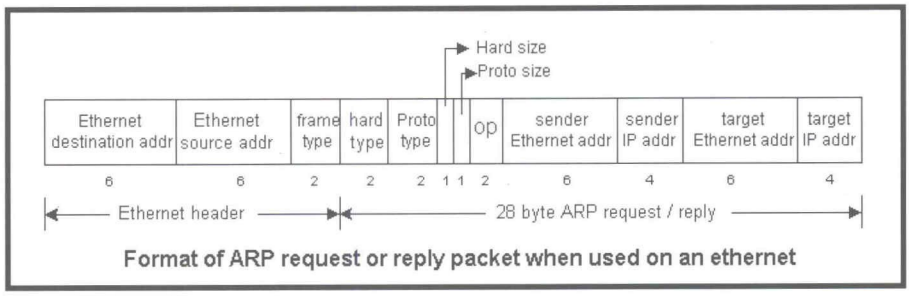
รูปที่ 10 โปรโตคอล ARP ห่อหุ้มด้วย Ethernet frame

- Operation Code มีขนาด 16 บิต ใช้ระบุว่าเป็นโปรโตคอล ARP หรือ RARP แบบ Request หรือ แบบ Reply ดังนี้

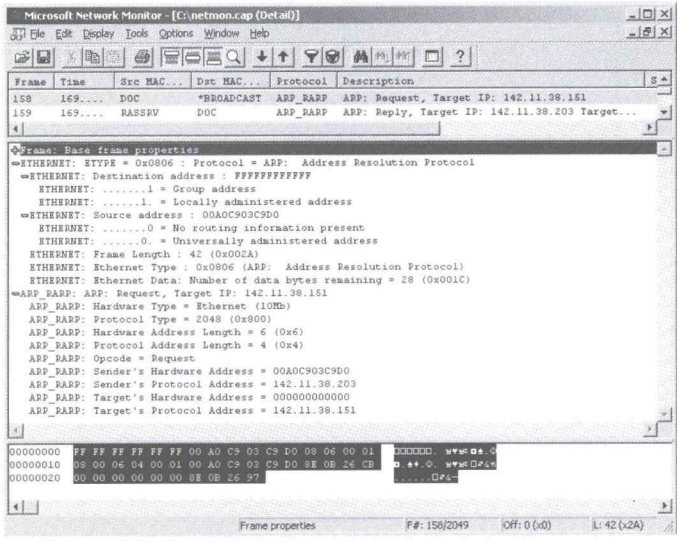
Operation Code	ความหมาย
1	ARP - Request
2	ARP - Reply
3	RARP - Request
4	RARP - Reply

- Sender Hardware Address มีขนาด 48 บิต ระบุ Mac Address ของผู้ส่ง
- Sender IP Address มีขนาด 32 บิต ระบุ IP Address ของผู้ส่ง
- Recipient Hardware Address มีขนาด 48 บิต ระบุ Mac Address ของผู้รับ
- Recipient IP Address มีขนาด 32 บิต ระบุ IP Address ของผู้รับ

จากการ Capture โปรโตคอล ARP ตามรูปที่ 13 แสดงถึงการส่ง ARP Request จากเครื่อง IP Address 142.11.38.203 Mac Address เท่ากับ 00A0C903C9D0 เป็นการส่งแบบ Broadcast โดยการระบุ Destination address เป็น FFFFFFFFFFFF และโปรโตคอล ARP Request นี้ต้องการทราบค่า Mac Address ของเครื่องที่มี IP Address เท่ากับ 142.11.38.151



รูปที่ 11
ขนาดความยาว (byte) ของโปรโตคอล ARP ใน Ethernet Frame (1 ไบต์ = 8 บิต)



รูปที่ 12
โปรโตคอล ARP หา Mac Address ของเครื่อง IP = 142.11.38.151

```
Frame: Base frame properties
ETHERNET: ETYPE = 0x0806 : Protocol = ARP:  Address Resolution Protocol
  ETHERNET: Destination address : FFFFFFFFFFFF  <= 1
     ETHERNET: .....1 = Group address
     ETHERNET: .....1. = Locally administered address
  ETHERNET: Source address : 00A0C903C9D0
     ETHERNET: .....0 = No routing information present
     ETHERNET: .....0. = Universally administered address
    ETHERNET: Frame Length : 42 (0x002A)
    ETHERNET: Ethernet Type : 0x0806 (ARP:  Address Resolution Protocol)
    ETHERNET: Ethernet Data: Number of data bytes remaining = 28 (0x001C)
ARP_RARP: ARP: Request, Target IP: 142.11.38.151
    ARP_RARP: Hardware Type = Ethernet (10Mb)
    ARP_RARP: Protocol Type = 2048 (0x800)
    ARP_RARP: Hardware Address Length = 6 (0x6)
    ARP_RARP: Protocol Address Length = 4 (0x4)
    ARP_RARP: Opcode = Request  <= 2
    ARP_RARP: Sender's Hardware Address = 00A0C903C9D0
    ARP_RARP: Sender's Protocol Address = 142.11.38.203
    ARP_RARP: Target's Hardware Address = 000000000000  <= 3
    ARP_RARP: Target's Protocol Address = 142.11.38.151
```

รูปที่ 13
โปรโตคอล ARP ถามหาค่า Mac Addr. ของเครื่องที่มี IP = 142.11.38.151

```
Frame: Base frame properties
ETHERNET: ETYPE = 0x0806 : Protocol = ARP:  Address Resolution Protocol
  ETHERNET: Destination address : 00A0C903C9D0  <= 1
     ETHERNET: .....0 = Individual address
     ETHERNET: .....0. = Universally administered address
  ETHERNET: Source address : 00E018992021
     ETHERNET: .....0 = No routing information present
     ETHERNET: .....0. = Universally administered address
    ETHERNET: Frame Length : 60 (0x003C)
    ETHERNET: Ethernet Type : 0x0806 (ARP:  Address Resolution Protocol)
    ETHERNET: Ethernet Data: Number of data bytes remaining = 46 (0x002E)
ARP_RARP: ARP: Reply, Target IP: 142.11.38.203 Target Hdwr Addr: 00A0C903C9D0
    ARP_RARP: Hardware Type = Ethernet (10Mb)
    ARP_RARP: Protocol Type = 2048 (0x800)
    ARP_RARP: Hardware Address Length = 6 (0x6)
    ARP_RARP: Protocol Address Length = 4 (0x4)
    ARP_RARP: Opcode = Reply  <= 2
    ARP_RARP: Sender's Hardware Address = 00E018992021
    ARP_RARP: Sender's Protocol Address = 142.11.38.151
    ARP_RARP: Target's Hardware Address = 00A0C903C9D0  <= 3
    ARP_RARP: Target's Protocol Address = 142.11.38.203
    ARP_RARP: Frame Padding
```

รูปที่ 14 โปรโตคอล ARP ที่ตอบกลับจากเครื่องที่มี IP = 142.11.38.151

จากรูปที่ 14 แสดงถึงการตอบโปรโตคอล ARP Request ของรูปที่ 13 ที่ต้องการทราบค่า Mac Address ของเครื่องที่มี IP Address เท่ากับ 142.11.38.151 โดยเครื่องที่มี IP Address 142.11.38.151 ได้ทำการส่ง ARP Reply ตอบกลับค่า Mac Address ของเครื่องตัวเองไปให้เครื่องที่ถามมา (IP Address 142.11.38.203 Mac Address 00A0C903c9D)

ส่งท้าย

โปรแกรม Network Monitor สามารถที่จะทำการ Capture โปรโตคอลอื่น ๆ ได้ด้วย เป็นต้นว่า IPX/SPX, NetBeui และถ้าคุณไม่ต้องการให้โปรโตคอลอื่น ๆ เข้ามารบกวนการศึกษาการทำงานของโปรโตคอล คุณอาจจะตั้งเน็ตเวิร์กใหม่ที่มีเฉพาะตัวส่งและตัวรับก็จะช่วยให้คุณได้เห็นโปรโตคอลที่ต้องการ Capture ได้สะดวกขึ้น